

REMARKS

Claims 6, 10, 12, 15, 19, 22, and 25 have been cancelled without prejudice. New claims 39-45 have been added to the application. As a result, claims 1-5, 7-9, 11, 13, 14, 16-18, 20, 21, 23, 24, 26-45 are now pending in the patent application. Claims 8, 13, 16-18, 21, 23, 28, 31-34, and 36 have been amended.

In the Office Action, claims 8, 14, 23, 31, and 36 are objected to under 37 C.F.R. §1.75 as being substantial duplicates of claims 6, 12, 19, 25, 28, respectively. A preliminary amendment to the claims in the present application was filed on November 26, 2001. The preliminary amendment inadvertently applied amendments to a set of claims that is different from the original set of claims filed in the application on September 7, 2000. The new claims and amendments to the claims including the cancellation of claims 6, 10, 12, 15, 19, 22, and 25 are submitted to produce a claim set that applies the intended amendments from the preliminary amendment and deletes any amendments that were unintentionally made to the original claims. Where convenient, claims containing unintentional amendments were simply cancelled and amended duplicates of the original claims were added as new claims. The amendments should resolve the duplication objection.

Reconsideration of the objection in view of the amendments is requested.

Claims 1-4, 8, 10, 11, 13-15, 17, 21-24, 26, 30-32, 34, 36, and 38 are rejected in the Office Action under 35 U.S.C. §102(e) as being anticipated by Gottfried (U.S. Patent No. 6,270,011). However, Gottfried does not show or teach the systems and methods of claims 1-4, 8, 10, 11, 13-15, 17, 21-24, 26, 30-32, 34, 36, and 38. Reconsideration and withdrawal of the rejection in view of the foregoing are requested.

The systems and methods of the present invention as claimed, for example, in claim 1 are directed towards authorizing purchase transaction over a computer network involving, among other things, electronically transmitting an account number that identifies a consumer's account over the network from a consumer location to an on-line merchant location, forwarding the account number electronically over the network from the on-line merchant location to a third party contractor location, determining at said third party contractor location an authentication token type associated with said account number, and prompting the consumer at the consumer location to electronically transmit an authentication token in accordance with said determined token type over the network to the third party

contractor location. With respect to the authentication token type, the specification of the application states the following:

"the third computer 20 next determines the type of authentication token required by the issuer of the consumer's ATM card (step 42). The authentication token may be, for example, a PIN, a biometric signature such as a fingerprint or retinal image, an authorization code stored on a smart card, a password, or a combination of the foregoing. In the preferred embodiment of the present invention, this determination is based on the ATM card number." Page 13, lines 17-23.
(emphasis added)

Gottfried does not, for example, show that an authentication token type associated with an account number is determined at third party contractor's location and further does not show the prompting of the consumer at the consumer location to electronically transmit an authentication token in accordance with said determined token type. Gottfried shows an Internet-based credit card authorization system that relies on fingerprint information from a user to authorize a user transaction with a website. In the Internet-based credit card authorization system of Gottfried, a user enters credit card information and sends a buy request via the user's PC to a store server; the store server contacts a credit card company database and notifies the database via the Internet to verify the credit card information for the purchase; the credit card company sends a request requesting fingerprint data from the user, and the user sends the fingerprint information via the Internet to the credit card company database using a PC and an adapter connected to the PC for reading and encrypting the information. Gottfield, column 8, line 60, to column 9, line 29. Gottfried further states that:

"[t]he Internet-based credit card authorization system . . . permits the safe and secure completion of purchase transactions via the Internet, with the purchase being made using encrypted personal fingerprint information. This insures a high level of security since the seller (via the website) knows that the buyer's identity has been validated." Gottfried, column 9, lines 30-35.
(emphasis added)

The method of claim 1 specifically involves determining at said third party contractor location an authentication token type associated with said account number and prompting the consumer at the consumer location to electronically transmit an authentication token in accordance with said determined token type over the network to the third party contractor location. Such features are not shown by Gottfried.

There is no such determination or prompting shown to be implemented in the Gottfried system. Gottfried shows only the use of a fingerprint by a user to authorize an Internet transaction. Gottfried emphasizes this point repeatedly and does not describe or suggest other techniques involving something other a fingerprint be used within the Gottfried system. As such, Gottfried does not show the explicit step of determining an authentication token type (e.g., one of a password, PIN, or biometric type). In Gottfried, the system is implemented only with fingerprint information and operates with the predetermined knowledge that authorization by the user is only to be via fingerprint. The execution of software code to determine an authentication token type in the Gottfried system would be contrary to the specific system configuration described by Gottfried. In addition, Gottfried does not show that a user is prompted to electronically transmit an authentication token in accordance with said determined token type because, as mentioned above, no such determination of token type is shown to be performed by the Gottfried system.

Moreover, Gottfried teaches away from the step of determining of an authentication type. In the discussion of authorization techniques mentioned in the summary of the invention and the detailed description of Gottfried, the techniques are limited only to the authorization of a transaction by a user via fingerprint. No other means other than the singular use of a fingerprint are described, which eliminates the need for the system to determine an authentication type for a transaction since the use of a fingerprint is the only one implemented. Moreover, the background section in Gottfried indicates that known systems (e.g., those using a password or a user ID) have drawbacks which the fingerprint based authorization techniques of Gottfried overcomes. Specifically, in the background section, Gottfried states that:

"[i]n existing credit card security systems, heavy reliance is placed on the possession of the card itself and identification numbers that the user must protect and remember. These identification techniques lead to problems if the card is stolen and the identification number is copied or forgotten. . . . The current practice used for purchases over the Internet is also subject to fraudulent activities The entire purchase transaction can be encrypted or not according to the country or company, using a private or public encryption key. The user may also provide a password or user ID, but if the key or password is discovered by another, it can be used for non-legitimate purchases, and fraudulent activities. Therefore, it would be desirable to provide a method of enhancing the security of credit card transactions conducted via point-of-sale or Internet purchase authorization systems, to eliminate the

potential for fraudulent activities by verifying the identity of user of the card, and to avoid the use of stolen credit cards by others." Gottfried, column 1, lines 30-34, column 2, lines 24-25 and lines 32-37. (emphasis added).

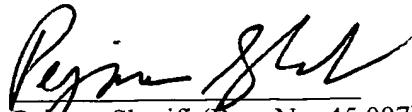
According, the systems and methods of independent claims 1, 23, 31, and 41 are not anticipated or obvious in view of Gottfried. Reconsideration and withdrawal of the rejection of claims 1, 23, 31, and 41 are requested.

Claims 2-4, 8, 10, 11, 13-15, 17, 21, 22, 24, 26, 30, 32, 34, 36, 38, and new claims 39-40 and 42-45, which each depend from one of claims 1, 23, 31, and 41, are allowable at least for the reasons set forth above regarding claims 1, 23, 31, and 41. Additionally, the dependent claims recite further features not disclosed or known in the prior art, particularly when considered in combination with the unique features of corresponding independent claims 1, 23, 31, and 41. Reconsideration and withdrawal of the rejection of claims 2-4, 8, 10, 11, 13-15, 17, 21, 22, 24, 26, 30, 32, 34, 36, and 38 are requested.

In the Office Action, claims 5, 7, 9, 16, 18, 20, 27, 29, 33, 35, and 37 are rejected under 35 U.S.C. §103(a) as being unpatentable over Gottfried. Claims 5, 7, 9, 16, 18, 20, 27, 29, 33, 35, and 37, which each depend from one of claims 1, 23, 31, and 41, are allowable at least for the reasons set forth above regarding claims 1, 23, 31, and 41. Additionally, the dependent claims recite further features not disclosed or known in the prior art, particularly when considered in combination with the unique features of corresponding independent claims 1, 23, 31, and 41. Reconsideration and withdrawal of the rejection of claims 5, 7, 9, 16, 18, 20, 27, 29, 33, 35, and 37 are requested.

For the foregoing reasons, Applicant submits that all of the claims are patentable over the cited art and respectfully requests an early indication of allowance. The Examiner is invited to contact the undersigned if any additional information is required.

Respectfully submitted,



Peiman Sharifi (Reg. No. 45,097)

For: Allan Fanucci (Ref. No. 30,256)

Customer No. 28765

Winston & Strawn LLP

(212) 294-6700